

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-228522

(43)Date of publication of application : 15.08.2003

(51)Int.Cl. G06F 12/14
G11B 20/10
H04L 9/10

(21)Application number : 2002-027138 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

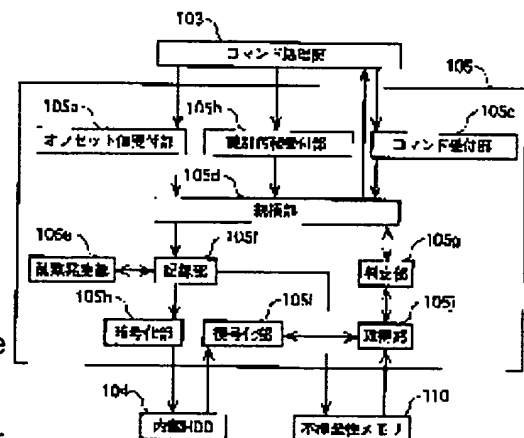
(22)Date of filing : 04.02.2002 (72)Inventor : ITO YOSHIKATSU
MURASE KAORU

(54) DIGITAL CONTENT MANAGEMENT DEVICE AND DIGITAL CONTENT MANAGEMENT PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data use position recorder and a data use position recording method that enable a movement of digital contents without causing loss of the digital contents while preventing unauthorized copying.

SOLUTION: When digital contents are recorded, a recording part 105f writes identification information on the digital contents and a random number generated by a random number generation part 105e into a nonvolatile memory 110 and a built-in HDD 104. When the digital contents are moved from the built-in HDD 104 to another recording medium, if the random number in the nonvolatile memory 110 and the random number in the built-in HDD 104 match, and a readout start position of the digital contents is larger than an offset value in the built-in HDD 104, a determination part 105g permits the movement of the digital contents and stores a readout end position of the digital contents in the built-in HDD 104 as a new offset value.



LEGAL STATUS

[Date of request for examination] 25.11.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2003-228522
(P2003-228522A)

(43)公開日 平成15年8月15日(2003.8.15)

(51)Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 1 1 B 20/10		G 1 1 B 20/10	H 5 D 0 4 4
H 0 4 L 9/10		H 0 4 L 9/00	6 2 1 Z 5 J 1 0 4

審査請求 未請求 請求項の数24 O L (全 17 頁)

(21)出願番号 特願2002-27138(P2002-27138)

(22)出願日 平成14年2月4日(2002.2.4)

(71)出願人 000005821

松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者 井藤 好克

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 村瀬 薫

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74)代理人 100090446

弁理士 中島 司朗

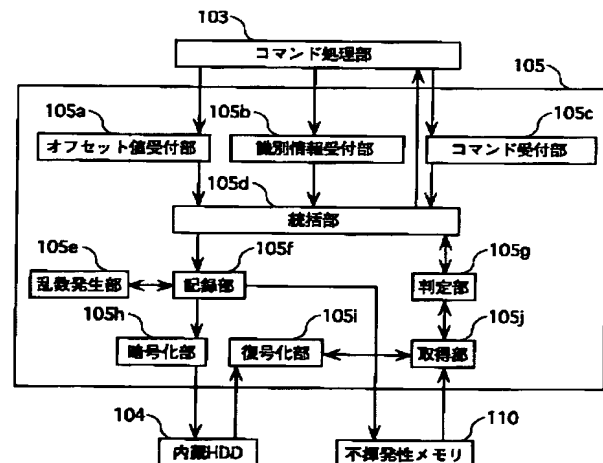
最終頁に続く

(54)【発明の名称】 デジタルコンテンツ管理装置およびデジタルコンテンツ管理プログラム

(57)【要約】

【課題】 不正コピーを防止しながら、デジタルコンテンツの喪失を招くことなくデジタルコンテンツの移動を可能にするデータ利用位置記録装置、及び、データ利用位置記録方法を提供することを目的とする。

【解決手段】 デジタルコンテンツを記録する際に、記録部105fはデジタルコンテンツの識別情報と乱数発生部105eが発生した乱数を、不揮発性メモリ110と内蔵HDD104に書き込んでおく。デジタルコンテンツを内蔵HDD104から他の記録媒体に移動する際には、判定部105gは不揮発性メモリ110の乱数と内蔵HDD104の乱数が一致し、かつデジタルコンテンツの読み出し開始位置が内蔵HDD104のオフセット値より大きいければ、デジタルコンテンツの移動を許可し、デジタルコンテンツの読み出し終了位置を新たなオフセット値として内蔵HDD104に格納する。



【特許請求の範囲】

【請求項 1】 デジタルコンテンツと当該デジタルコンテンツに対応する管理情報とを記録する第 1 の記録手段と、

前記管理情報を記録する第 2 の記録手段と、
デジタルコンテンツの利用に先立って、前記第 1 の記録手段にて記録されている管理情報と前記第 2 の記録手段にて記録されている管理情報とを照合して、前記デジタルコンテンツの利用の可否を判定する管理情報判定手段と、

前記管理情報判定手段にて利用可と判定されたデジタルコンテンツが利用されるに際して、前記第 1 の記録手段にて記録されている管理情報と前記第 2 の記録手段にて記録されている管理情報とを変更する管理情報更新手段とを備えることを特徴とするデジタルコンテンツ管理装置。

【請求項 2】 前記第 1 の記録手段にて記録する管理情報を暗号化する管理情報暗号化手段と、
前記第 1 の記録手段から読み出された管理情報を復号化する管理情報復号化手段とを備え、
前記第 1 の記録手段は、前記管理情報暗号化手段にて暗号化された管理情報を記録し、
前記管理情報判定手段は、前記管理情報復号化手段にて復号化された管理情報を用いて前記照合を行なうことを特徴とする請求項 1 に記載のデジタルコンテンツ管理装置。

【請求項 3】 前記第 1 の記録手段にて記録する管理情報を符号化する第 1 の符号化手段と、
前記第 2 の記録手段から読み出された管理情報を符号化する第 2 の符号化手段とを備え、
前記第 1 の記録手段は、前記第 1 の符号化手段にて符号化された管理情報を記録し、
前記管理情報判定手段は、前記第 2 の符号化手段にて符号化された管理情報を用いて前記照合を行なうことを特徴とする請求項 1 に記載のデジタルコンテンツ管理装置。

【請求項 4】 前記第 1 の記録手段から読み出された管理情報を符号化する第 1 の符号化手段と、
前記第 2 の記録手段にて記録する管理情報を符号化する第 2 の符号化手段とを備え、
前記第 2 の記録手段は、前記第 2 の符号化手段にて符号化された管理情報を記録し、
前記管理情報判定手段は、前記第 1 の符号化手段にて符号化された管理情報を用いて前記照合を行なうことを特徴とする請求項 1 に記載のデジタルコンテンツ管理装置。

【請求項 5】 デジタルコンテンツ中の利用位置を取得する位置取得手段と、
デジタルコンテンツ中の利用位置の末尾位置を記録する末尾位置記録手段と、

前記末尾位置記録手段にて記録されているデジタルコンテンツ中の利用位置の末尾位置と、位置取得手段にて取得されたデジタルコンテンツ中の利用位置とを比較して、デジタルコンテンツの利用の可否を判定する位置判定手段と、

前記管理情報判定手段と前記位置判定手段とがデジタルコンテンツを利用可と判定したときのみ、デジタルコンテンツを利用可と判定する最終判定手段とを備えることを特徴とする請求項 1 から請求項 4 のいずれかに記載のデジタルコンテンツ管理装置。

【請求項 6】 前記末尾位置記録手段は、前記第 1 の記録手段にて前記デジタルコンテンツ中の利用位置の末尾位置を記録することを特徴とする請求項 5 に記載のデジタルコンテンツ管理装置。

【請求項 7】 前記末尾位置記録手段は、前記デジタルコンテンツ中の利用位置の末尾位置を暗号化して記録することを特徴とする請求項 5 または請求項 6 に記載のデジタルコンテンツ管理装置。

【請求項 8】 前記デジタルコンテンツは 1 以上の部分データからなっており、
前記デジタルコンテンツ中の利用位置は、前記デジタルコンテンツの先頭からの前記部分データの順序情報により示されることを特徴とする請求項 5 に記載のデジタルコンテンツ管理装置。

【請求項 9】 乱数を発生させる乱数発生手段を備え、前記管理情報は前記乱数発生手段が発生させた乱数を含んでいることを特徴とする請求項 1 から請求項 8 のいずれかに記載のデジタルコンテンツ管理装置。

【請求項 10】 前記デジタルコンテンツを識別する識別情報を取得する識別情報取得手段を備え、
前記管理情報は前記識別情報を含んでいることを特徴とする請求項 1 から請求項 9 のいずれかに記載のデジタルコンテンツ管理装置。

【請求項 11】 前記識別情報は、対応するデジタルコンテンツのハッシュ値を含み、
前記第 1 の記録手段から読み出したデジタルコンテンツのハッシュ値と前記第 2 の記録手段から読み出した管理情報に含まれているハッシュ値を照合してデジタルコンテンツの利用の可否を判定するハッシュ値照合手段を備えることを特徴とする請求項 10 に記載のデジタルコンテンツ管理装置。

【請求項 12】 前記第 1 の記録手段は、前記デジタルコンテンツを暗号鍵を用いて暗号化して記録し、
前記識別情報は、前記暗号鍵を含み、
前記第 1 の記録手段から読み出した前記識別情報に含まれている暗号鍵と前記第 2 の記録手段から読み出した前記識別情報に含まれている暗号鍵とを照合してデジタルコンテンツの利用の可否を判定する暗号鍵照合手段を備えることを特徴とする請求項 10 に記載のデジタルコンテンツ管理装置。

【請求項 13】 前記第 2 の記録手段は不揮発性メモリであることを特徴とする請求項 1 から請求項 12 のいずれかに記載のデジタルコンテンツ管理装置。

【請求項 14】 デジタルコンテンツと当該デジタルコンテンツに対応する管理情報とを記録する第 1 の記録ステップと、
前記管理情報を記録する第 2 の記録ステップと、
前記デジタルコンテンツが利用される際に、前記第 1 の記録ステップにて記録された管理情報と前記第 2 の記録ステップにて記録された管理情報とを更新する管理情報更新ステップと、
前記第 1 の記録ステップにて記録された管理情報と前記第 2 の記録ステップにて記録された管理情報とを照合して、前記デジタルコンテンツの利用の可否を判定する管理情報判定ステップとを備えることを特徴とするデジタルコンテンツ管理プログラム。

【請求項 15】 前記第 1 の記録ステップにて記録する管理情報を暗号化する管理情報暗号化ステップと、
前記第 1 の記録ステップにて記録された管理情報を復号化する管理情報復号化ステップとを備えることを特徴とする請求項 14 に記載のデジタルコンテンツ管理プログラム。

【請求項 16】 前記第 1 の記録ステップにて記録する管理情報を符号化する第 1 の符号化ステップと、
前記第 2 の記録ステップにて記録された管理情報を符号化する第 2 の符号化ステップとを備えることを特徴とする請求項 14 に記載のデジタルコンテンツ管理プログラム。

【請求項 17】 前記第 1 の記録ステップにて記録された管理情報を符号化する第 1 の符号化ステップと、
前記第 2 の記録ステップにて記録する管理情報を符号化する第 2 の符号化ステップとを備えることを特徴とする請求項 14 に記載のデジタルコンテンツ管理プログラム。

【請求項 18】 デジタルコンテンツの利用位置を取得する位置取得ステップと、
デジタルコンテンツの利用位置の末尾位置を記録する末尾位置記録ステップと、
前記末尾位置記録ステップにて記録されたデジタルコンテンツの利用位置の末尾位置と、位置取得ステップにて取得されたデジタルコンテンツの利用位置とを比較して、デジタルコンテンツの利用の可否を判定する位置判定ステップと、
前記管理情報判定ステップと前記位置判定ステップとがデジタルコンテンツを利用可と判定したときのみ、デジタルコンテンツを利用可と判定する最終判定ステップとを備えることを特徴とする請求項 14 から請求項 17 のいずれかに記載のデジタルコンテンツ管理プログラム。

【請求項 19】 前記末尾位置記録ステップは、前記デジタルコンテンツ中の利用位置の末尾位置を暗号化して

記録することを特徴とする請求項 18 に記載のデジタルコンテンツ管理プログラム。

【請求項 20】 前記デジタルコンテンツは 1 以上の部分データからなっており、
前記デジタルコンテンツの利用位置は、前記デジタルコンテンツの先頭からの前記部分データの順序情報により示されることを特徴とする請求項 18 に記載のデジタルコンテンツ管理プログラム。

【請求項 21】 前記管理情報として乱数を発生させる乱数発生ステップを備えることを特徴とする請求項 14 から請求項 20 のいずれかに記載のデジタルコンテンツ管理プログラム。

【請求項 22】 前記デジタルコンテンツを識別する識別情報を取得する識別情報取得ステップを備え、
前記管理情報は前記識別情報を含んでいることを特徴とする請求項 14 から請求項 21 のいずれかに記載のデジタルコンテンツ管理プログラム。

【請求項 23】 前記識別情報は、対応するデジタルコンテンツのハッシュ値を含み、
前記第 1 の記録ステップにて記録されたデジタルコンテンツのハッシュ値と前記第 2 の記録ステップにて記録された管理情報に含まれているハッシュ値を照合してデジタルコンテンツの利用の可否を判定するハッシュ値照合ステップを備えることを特徴とする請求項 22 に記載のデジタルコンテンツ管理プログラム。

【請求項 24】 前記第 1 の記録ステップは、前記デジタルコンテンツを暗号鍵を用いて暗号化して記録し、
前記識別情報は、前記暗号鍵を含み、
前記第 1 の記録ステップにて記録された前記識別情報に含まれている暗号鍵と前記第 2 の記録ステップにて記録された前記識別情報に含まれている暗号鍵とを照合してデジタルコンテンツの利用の可否を判定する暗号鍵照合ステップを備えることを特徴とする請求項 22 に記載のデジタルコンテンツ管理プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタルコンテンツの不正利用を防止する為にデジタルコンテンツの管理を行なうデジタルコンテンツ管理装置およびデジタルコンテンツ管理プログラムに関し、特に、不正利用を防止しつつユーザの利便性を高める技術に関する。

【0002】

【従来の技術】近年、BS デジタル放送の開始に伴って、映画作品等がデジタルコンテンツとして広く配信されるようになってきた。デジタルコンテンツは複製が容易であり、また、インターネットその他の媒体を介して簡単に造り取りができるため、海賊行為や不正な複製の再配信に対する懸念が高まっており、これに呼応してデジタルコンテンツを保護するための技術開発が進められている。

【0003】このようなデジタルコンテンツの保護技術に関する規格として、例えば、DTCP (Digital Transmission Content Protection) がある。DTCPは、デジタルコンテンツをデジタル転送する際に、デジタルコンテンツを暗号化する等して不正なコピーを防止する技術である。DTCPのようなデジタルコンテンツ保護技術においては、デジタルコンテンツに、「Copy No More」、「Copy one Generation」等のコピー制御情報 (CCI: Copy Control Information) を付与する。

【0004】「Copy No More」はデジタルコンテンツのコピーが禁止されている旨を表す。また、「Copy one Generation」はデジタルコンテンツのコピーが1回だけ許されていることを表す。従って、コピー制御情報として「Copy one Generation」を付与されたデジタルコンテンツをコピーすると、コピーによって新たに得られたデジタルコンテンツにはコピー制御情報として「Copy No More」が付与される。

【0005】このようなデジタルコンテンツ保護技術をデジタルビデオレコーダ等の機器が採用すれば、デジタルコンテンツの不正コピーの防止するのに与って力がある。

【0006】

【発明が解決しようとする課題】しかしながら、コピー制御情報として「Copy No More」が付与されたデジタルコンテンツであっても、他の記録媒体への移動が必要となる場合がある。例えば、デジタルテレビに内蔵されているHDD (Hard Disk Drive) に記録されているデジタルコンテンツをDVD-RAMにコピーし、愛蔵版として保存しておきたいような場合である。この際、当然に内蔵HDDから当該デジタルコンテンツは再生できない状態にされなければならない。

【0007】かかる場合に、内蔵HDDからDVD-RAMにデジタルコンテンツの全体をコピーした後に、内蔵HDDに記録されているデジタルコンテンツを消去する等してデジタルコンテンツを無効化する、すなわちデジタルコンテンツを利用できない状態にする方法が考えられる。しかしながら、デジタルコンテンツの移動に先立ってデジタルテレビから内蔵HDDを取り出し、これをパーソナルコンピュータに接続してバックアップを作成し、デジタルコンテンツを移動した後にバックアップしておいたデータを内蔵HDDに戻すといった操作をされると、デジタルコンテンツを何回でも移動できるようになり、不正コピーを防止することが出来ない。

【0008】また、デジタルコンテンツの移動中に電源断等の原因により移動元のデジタルコンテンツと移動先のデジタルコンテンツとのいずれもが損なわれ、デジタ

ルコンテンツとして利用できなくなるのでは、デジタルコンテンツの利用者にとって不便である。また、このようにして利用できなくなったデジタルコンテンツを再度入手するために出費が必要な場合には経済的な損失も発生する。

【0009】本発明は、上記のような問題に鑑みてなされたものであって、不正コピーを防止しながら、デジタルコンテンツの喪失を招くことなくデジタルコンテンツの移動を可能にするデータ利用位置記録装置、及び、データ利用位置記録方法を提供することを目的とする。

【0010】

【課題を解決するための手段】上記の目的を達成するため、本発明に係るデータ利用位置記録装置は、デジタルコンテンツと当該デジタルコンテンツに対応する管理情報とを記録する第1の記録手段と、前記管理情報を記録する第2の記録手段と、デジタルコンテンツの利用に先立って、前記第1の記録手段にて記録されている管理情報と前記第2の記録手段にて記録されている管理情報とを照合して、前記デジタルコンテンツの利用の可否を判定する管理情報判定手段と、前記管理情報判定手段にて利用可と判定されたデジタルコンテンツが利用されるに際して、前記第1の記録手段にて記録されている管理情報と前記第2の記録手段にて記録されている管理情報とを変更する管理情報更新手段とを備えることを特徴とする。

【0011】このようにすれば、デジタルコンテンツを移動させる前に内蔵HDDのバックアップを作成し、移動後にバックアップしておいたデジタルコンテンツを内蔵HDDに戻す操作をされても、前記第1の記録手段にて記録されている管理情報と前記第2の記録手段にて記録されている管理情報との照合により検出できるので、不正コピーを防止することが出来る。

【0012】また、前記第1の記録手段にて記録する管理情報を暗号化する管理情報暗号化手段と、前記第1の記録手段から読み出された管理情報を復号化する管理情報復号化手段とを備え、前記第1の記録手段は、前記管理情報暗号化手段にて暗号化された管理情報を記録し、前記管理情報判定手段は、前記管理情報復号化手段にて復号化された管理情報を用いて前記照合を行なうことを特徴とする。このようにすれば、管理情報を改竄され難くなるので、上述のような不正コピー対策を更に強化することができる。

【0013】また、前記第1の記録手段にて記録する管理情報を符号化する第1の符号化手段と、前記第2の記録手段から読み出された管理情報を符号化する第2の符号化手段とを備え、前記第1の記録手段は、前記第1の符号化手段にて符号化された管理情報を記録し、前記管理情報判定手段は、前記第2の符号化手段にて符号化された管理情報を用いて前記照合を行なうとしても良い。このようにすれば、上記と同様に、管理情報が改竄され

難くなるので、不正コピーの防止を更に強化することができる。

【0014】また、前記第1の記録手段から読み出された管理情報を符号化する第1の符号化手段と、前記第2の記録手段にて記録する管理情報を符号化する第2の符号化手段とを備え、前記第2の記録手段は、前記第2の符号化手段にて符号化された管理情報を記録し、前記管理情報判定手段は、前記第1の符号化手段にて符号化された管理情報を用いて前記照合を行なうとしても良い。

【0015】また、デジタルコンテンツ中の利用位置を取得する位置取得手段と、デジタルコンテンツ中の利用位置の末尾位置を記録する末尾位置記録手段と、前記末尾位置記録手段にて記録されているデジタルコンテンツ中の利用位置の末尾位置と、位置取得手段にて取得されたデジタルコンテンツ中の利用位置とを比較して、デジタルコンテンツの利用の可否を判定する位置判定手段と、前記管理情報判定手段と前記位置判定手段とがデジタルコンテンツを利用可と判定したときのみ、デジタルコンテンツを利用可と判定する最終判定手段とを備えることを特徴とする。このようにすれば、デジタルコンテンツの利用位置を記録し、この記録に基づいて利用の可否を判定すれば、デジタルコンテンツの移動が電源断等の原因により中断しても、当該デジタルコンテンツの移動未完了の部分が利用不可とならず、デジタルコンテンツの喪失を回避することができる。

【0016】なお、上記に際して、前記末尾位置記録手段は、前記第1の記録手段にて前記デジタルコンテンツ中の利用位置の末尾位置を記録するとしても良いし、更に、前記末尾位置記録手段は、前記デジタルコンテンツ中の利用位置の末尾位置を暗号化して記録するとしても良い。なお、デジタルコンテンツの利用位置を記録するにあたっては、例えば、前記デジタルコンテンツは1以上の部分データからなっており、前記デジタルコンテンツ中の利用位置は、前記デジタルコンテンツの先頭からの前記部分データの順序情報により示されるとすれば良い。

【0017】また、乱数を発生させる乱数発生手段を備え、前記管理情報は前記乱数発生手段が発生させた乱数を含んでいることを特徴とする。このようにすれば、デジタルコンテンツの不正利用者による管理情報の改竄が困難となるので、不正コピーの防止を強化することができる。また、前記デジタルコンテンツを識別する識別情報を取得する識別情報取得手段を備え、前記管理情報は前記識別情報を含んでいることを特徴とする。このようにすれば、例えば、デジタルテレビの内蔵HDDに格納されているデジタルコンテンツを別のデジタルコンテンツに書き換えて、当該別のデジタルコンテンツが不正利用されるのを防止することができる。

【0018】ここで、前記識別情報は、対応するデジタルコンテンツのハッシュ値を含み、前記第1の記録手段

から読み出したデジタルコンテンツのハッシュ値と前記第2の記録手段から読み出した管理情報に含まれているハッシュ値を照合してデジタルコンテンツの利用の可否を判定するハッシュ値照合手段を備えるとすれば、かかる不正利用をより確実に検出して、これを防止することができる。

【0019】また、前記第1の記録手段は、前記デジタルコンテンツを暗号鍵を用いて暗号化して記録し、前記識別情報は、前記暗号鍵を含み、前記第1の記録手段から読み出した前記識別情報に含まれている暗号鍵と前記第2の記録手段から読み出した前記識別情報に含まれている暗号鍵とを照合してデジタルコンテンツの利用の可否を判定する暗号鍵照合手段を備えるとしても良い。

【0020】また、前記第2の記録手段は不揮発性メモリであるとするれば、回路基板から取り外して内容を読み出しや改竄したりするのが困難であるので、上記において、前記第2の記録手段にて記録された管理情報の読み出しや改竄が困難となり、デジタルコンテンツの不正利用の防止を強化することができる。また、本発明に係るデジタルコンテンツ管理プログラムは、コンピュータをして上記デジタルコンテンツ管理装置のような動作をさせることができるので、コンピュータに上記デジタルコンテンツ管理装置と同様の効果を奏させることができる。

【0021】

【発明の実施の形態】以下、本発明に係るデータ利用位置記録装置の実施の形態について、BSデジタルテレビ受像機（以下、単に「デジタルテレビ」という。）を例にとり、図面を参照しながら説明する。本実施の形態に係るデジタルテレビは、デジタル放送されたデジタルコンテンツを受信して内蔵HDDに蓄積し、当該デジタルコンテンツの保護を図りながら、当該デジタルコンテンツをモニタに映像表示させたり、他の記録媒体に向けて転送したりする装置である。

【0022】（全体構成）図1は、本実施の形態に係るデジタルテレビの構成を示す機能ブロック図である。図1に示すように、デジタルテレビ1はチューナ部102やモニタ部106等を備えている。また、デジタルテレビ1にはBSデジタル放送の電波を受信するためのBSデジタル用アンテナ3が接続されていると共に、受信したデジタルコンテンツをDVDに記録するためのDVDレコーダ4がIEEE1394インタフェースにて接続されている。

【0023】デジタルテレビ1は、皿型のBSデジタル用アンテナ3を介して、放送衛星2からBSデジタル放送を受信する。チューナ部102はBSデジタル放送された放送信号を受信、復調してトランスポートストリームを生成する。チューナ部102は、トランスポートストリームに含まれているトランスポートストリームパケット（以下、「TSパケット」という。）のうち、コマ

ンド処理部103が指定したチャンネルに該当するTSパケット以外のTSパケットは廃棄する。

【0024】コマンド処理部103が指定したチャンネルに該当するTSパケットの中には、契約者以外の者が視聴するのを防止するためにスクランブルがかけられているTSパケットもある。チューナ部102はトランスポートストリームに含まれている制御情報を参照して、スクランブルがかけられているTSパケットについては、カードリーダー部（以下、「カードR/W部」という。）101に対してスクランブルを解除するための復号鍵を要求する。

【0025】カードR/W部101はいわゆるCAS（Conditional Access System）カードを参照して該当する復号鍵を読み出して、チューナ部102に復号鍵を返信する。CASカードに該当する復号鍵がなければ、カードR/W部101はその旨をチューナ部102に通知する。チューナ部102はカードR/W部101から復号鍵が返信されたのであれば、当該復号鍵を用いてTSパケットのスクランブルを解除し、MPEGストリームとなす。そして、チューナ部102はコマンド処理部103からの指示に応じて、当該MPEGストリームを暗号処理部108とMPEGデコーダ107とのいずれか一方、またはこれら両方に向けて出力する。

【0026】カードR/W部101から復号鍵がない旨の応答があった場合には、チューナ部102はスクランブル解除の処理を実行することなく、当該TSパケットを廃棄する。また、そもそもスクランブルがかけられていないTSパケットについては、チューナ部102はカードR/W部101に問い合わせることなく、そのままMPEGストリームとなし、コマンド処理部103からの指示に従って暗号処理部108やMPEGデコーダ107に向けて出力する。

【0027】コマンド処理部103が暗号処理部108に出力すべきTSパケットのチャンネルとMPEGデコーダ107に出力すべきTSパケットのチャンネルとして相異なるチャンネルを指定した場合、チューナ部102はこの指定に従って、対応するチャンネルに係るMPEGストリームを暗号処理部108とMPEGデコーダ107とのそれぞれに対して出力する。これによって、いわゆる裏番組を内蔵HDD104に録画することが可能となる。

【0028】コマンド処理部103は、リモートコントローラまたは操作パネル（いずれも不図示）からコマンドを受け付けて、当該コマンドに応じた指示をチューナ部102、暗号処理部108またはデータ管理部105に発する。すなわち、コマンド処理部103はチューナ部102に対しては受信するチャンネルを指定する。このとき併せて、当該チャンネルに係るMPEGストリームの出力先として暗号処理部108とMPEGデコーダ1

07とのいずれか一方、またはこれら両方を指定する。

【0029】また、暗号処理部108に対しては、デジタルコンテンツの識別情報と当該デジタルコンテンツ中の読み出し開始位置（以下、「オフセット値」という。）とを指定して、当該デジタルコンテンツを内蔵HDD104から読み出せと指示する。このとき併せて、読み出したデジタルコンテンツに係るMPEGストリームの出力先としてMPEGデコーダ107と出力処理部109とのいずれか一方、またはこれら両方を指定する。尚、本実施の形態において、オフセット値とはデジタルコンテンツを構成するTSパケットを当該デジタルコンテンツの先頭から順に番号付けした場合の、その番号をいう。

【0030】データ管理部105に対しては、コマンド処理部103は3通りの動作をする。1つは、デジタルコンテンツを内蔵HDD104に記録するとの通知である。すなわち、コマンド処理部103はデータ管理部105に対してチューナ部102からのMPEGストリームを、暗号処理部108を介して内蔵HDD104に記録するとの通知を出す。この際、コマンド処理部103はデータ管理部105に対してデジタルコンテンツの識別情報を通知する。この識別情報は、例えば、コマンド処理部103が前記リモートコントローラや操作パネルを介して受け付けるとしても良い。

【0031】2番目は、内蔵HDD104に記録されたデジタルコンテンツを読み出す際の指示である。すなわち、コマンド処理部103はデータ管理部105に対してデジタルコンテンツの識別情報とオフセット値とを通知して、当該デジタルコンテンツを内蔵HDD104から読み出すことの可否を問い合わせる。この問い合わせに対して、データ管理部105から読み出しても良いとの応答を得た場合、コマンド処理部103は、暗号処理部108に対して、当該デジタルコンテンツの識別情報を通知して、当該デジタルコンテンツを内蔵HDD104から読み出し、復号化し、出力処理部109に向けて出力するように指示する。

【0032】暗号処理部108は、チューナ部102から受け付けたMPEGストリームに係るデジタルコンテンツに付加されているコピー制御情報が「Copy One Generation」である場合には、コピー制御情報を「Copy No More」に変更した後、当該デジタルコンテンツを暗号化して内蔵HDD104に格納する。暗号処理部108は、コピー制御情報として「Copy No More」が付加されているデジタルコンテンツは内蔵HDD104に格納しない。

【0033】また、暗号処理部108は、コマンド処理部103からデジタルコンテンツの識別情報とオフセット値との指定を伴って、内蔵HDD104から当該デジタルコンテンツを読み出せという指示を受け付けると、指定されたデジタルコンテンツを内蔵HDD104から

読み出して復号化し、MPEGストリームを生成する。そして、暗号処理部108は、コマンド処理部103からの指示に従って、当該MPEGストリームをMPEGデコーダ107と出力処理部109とのいずれか一方、またはこれら両方に向けて出力する。

【0034】内蔵HDD104は、暗号処理部108やデータ管理部105からのアクセスを受け付けてデジタルコンテンツ等を記録したり、読み出したりする。また、MPEGデコーダ107は、チューナ部102から受け付けたMPEGストリームを復号化して映像信号と音声信号とを生成し、モニタ部106に向けて出力する。モニタ部106はMPEGデコーダ107から映像信号と音声信号とを受け付けて、映像出力すると共に付属のスピーカからは音声を出力する。

【0035】データ管理部105は、デジタルコンテンツを内蔵HDD104に記録する際にその管理情報を不揮発性メモリ110に記録することによって、内蔵HDD104からデジタルコンテンツを読み出す際に前記管理情報を参照して、内蔵HDD104に格納されているデジタルコンテンツの正当性を確認する。データ管理部105は、コマンド処理部103からのデジタルコンテンツの識別情報の通知を受け付けて、当該通知に係るデジタルコンテンツを管理するための後述のような管理情報を内蔵HDD104と不揮発性メモリ110との両方に記録する。

【0036】またこれとは別に、データ管理部105は、コマンド処理部103から所定のデジタルコンテンツについて内蔵HDD104からの読み出しの可否の問い合わせを受け付けると、当該デジタルコンテンツに係る前記管理情報を内蔵HDD104と不揮発性メモリ110とのそれぞれから読み出して、これらを照合する。そして、データ管理部105は、その照合結果に応じて読み出しの可否を判定し、コマンド処理部103に判定結果を通知する。

【0037】出力処理部109は、暗号処理部108からMPEGストリームを受け付けると、当該デジタルコンテンツをDTP規格やIEEE1394規格にて定められた手順に従ってDVDレコーダ4に送信する。

(データ管理部105の構成) データ管理部105について更に詳しく説明する。図2は、データ管理部105の構成を示す機能ブロック図である。図2に示すように、データ管理部105はオフセット値受付部105aや識別情報受付部105b、コマンド受付部105c等の機能ブロックから成っている。オフセット値受付部105aは内蔵HDD104に格納されているデジタルコンテンツを読み出すためのオフセット値をコマンド処理部103から受け付ける機能ブロックである。

【0038】識別情報受付部105bは、デジタルコンテンツを識別するための識別情報をコマンド処理部103から受け付ける。コマンド受付部105cは、処理の

種別、すなわち記録、再生、移動のうちのいずれの処理が要求されているかを示すコマンドをコマンド処理部103から受け付ける。統括部105dは、コマンド受付部105cにて受け付けたコマンドに応じて、記録部105fや判定部105gに処理を振り分ける。また、統括部105dは、判定部105gから通知された判定結果をコマンド処理部103に対して通知し、或いは、当該判定結果に応じて記録部105fに処理を要求する。

【0039】記録部105fは、統括部105dからデジタルコンテンツの識別情報とオフセット値とを受け付けると、乱数発生部105eに要求して乱数を取得する。そして、記録部105fは、デジタルコンテンツの識別情報、オフセット値および乱数を不揮発性メモリ110に記録する。また、記録部105fは、暗号化部105hにデジタルコンテンツの識別情報、オフセット値および乱数を引き渡して、これらを内蔵HDD104に記録するように要求する。暗号化部105hは、記録部105fから当該要求を受け付けると、デジタルコンテンツの識別情報、オフセット値および乱数を暗号化して内蔵HDD104に記録する。

【0040】判定部105gは、統括部105dからデジタルコンテンツの識別情報とオフセット値とを受け付けると、当該識別情報を取得部106jに引き渡して、対応する乱数を内蔵HDD104と不揮発性メモリ110との各々から読み出すように要求する。判定部105gは取得部106jから前記識別情報等に対応する乱数を受け付けると、これらを照合して一致しているか否かを判定する。また、判定部105gは、統括部105dから受け付けたオフセット値と内蔵HDD104から読み出されたオフセット値とを、内蔵HDD104から読み出されたオフセット値が統括部105dから受け付けたオフセット値以下であるか否かを判定する。

【0041】そして、前記乱数が互いに一致し、かつ、内蔵HDD104から読み出されたオフセット値が統括部105dから受け付けたオフセット値以下である場合には、判定部105gは判定結果としてデジタルコンテンツ読み出し可と統括部105dに通知する。さもなければ、判定部105gは、デジタルコンテンツ読み出し不可と統括部105dに通知する。

【0042】取得部106jは、判定部105gからデジタルコンテンツの識別情報とオフセット値とを受け付けると、内蔵HDD104からこれら識別情報等に対応するオフセット値と乱数とを読み出すように復号化部105iに要求する。そして、取得部106jは、復号化部105iからオフセット値と乱数とを受け取ると、当該オフセット値と乱数とを判定部105gに引き渡す。また、この処理と併せて、取得部106jは、不揮発性メモリ110からも前記識別情報等に対応する乱数を読み出して、これも判定部105gに引き渡す。

【0043】乱数発生部105eは、記録部105fの

要求に応じて、公知のアルゴリズムに従って乱数を発生させ、これを記録部105fに引き渡す。また、暗号化部105hと復号化部105iは公知のアルゴリズムに従って暗号化と復号化の処理を遂行する。

(データ管理部105の動作) 次に、データ管理部105の動作について図面を参照しながら説明する。上述のように、データ管理部105はコマンド処理部からの要求に応じて3種類の動作を行なう。すなわち、記録、再生、移動である。図3は、データ管理部105の動作について、そのメインルーチンを示すフローチャートである。図3に示すように、データ管理部105は、コマンド処理部103からのコマンドをコマンド受付部105cにて受け付ける(ステップS1)。コマンド受付部105cは受け付けたコマンドを統括部105dに引き渡す。

【0044】統括部105dは、コマンド受付部105cからコマンドを受け取ると、当該コマンドを参照して次に実行すべき処理を決定する。すなわち、受け取ったコマンドが記録コマンドであれば(ステップS2: Yes)、記録処理を実行する(ステップS3)。受け取ったコマンドが記録コマンドではなくて(ステップS2: No)、再生コマンドならば(ステップS4: Yes)、統括部105dは再生処理を実行する(ステップS5)。

【0045】統括部105dは、受け取ったコマンドが再生コマンドでもなくて(ステップS4: No)、移動コマンドであれば(ステップS6: Yes)移動処理を実行する(ステップS7)。ステップS3、S5、S7の処理を終了した後、或いは受け取ったコマンドが記録コマンドでも、再生コマンドでも、移動コマンドでもない場合には(ステップS6: No)、統括部105dはステップS1に戻って処理を繰り返す。

【0046】以下、データ管理部105が実行する記録処理、再生処理および移動処理について更に詳しく説明する。

(1) 記録処理

図4は、データ管理部105が実行する記録処理について処理の流れを示したフローチャートである。図4に示すように、データ管理部105は、コマンド処理部103からの識別情報を識別情報受付部105bにて受け付ける(ステップS301)。当該識別情報は内蔵HDD104に記録すべきデジタルコンテンツと後述の乱数とを対応付けるための情報である。統括部105dは、識別情報受付部105bから識別情報を受け取ると、当該識別情報を記録部105fに引き渡すと共にオフセット値としてゼロを記録部105fに引き渡す。

【0047】記録部105fは、統括部105dから識別情報とオフセット値を受け取ると、乱数発生部105eに対して乱数を発生させるように要求する。乱数発生部105eは、記録部105fからの要求に応じて乱数

を発生させる(ステップS302)。そして、乱数発生部105eは、発生させた乱数を記録部105fに引き渡す。

【0048】記録部105fは、乱数発生部105eから乱数を受け取ると、当該乱数と統括部105dから受け取った識別情報とを不揮発性メモリ110に書き込む(ステップS303)。また、記録部105fは、前記識別情報、乱数およびオフセット値を暗号化部105hに引き渡して内蔵HDD104に格納するように要求する。暗号化部105hは、記録部105fから受け取った識別情報、乱数およびオフセット値を暗号化する(ステップS304)。そして、暗号化部105hは、暗号化した識別情報、乱数およびオフセット値を内蔵HDD104に書き込む(ステップS305)。

【0049】(2) 再生処理

図5は、データ管理部105が実行する再生処理について処理の流れを示したフローチャートである。図5に示すように、データ管理部105は、コマンド処理部103からの識別情報を識別情報受付部105bにて受け付ける(ステップS501)。更に、データ管理部105は、コマンド処理部103からのオフセット値をオフセット値受付部105aにて受け付ける(ステップS502)。

【0050】統括部105dは、識別情報受付部105bから識別情報を受け取り、オフセット値受付部105aからオフセット値を受け取ると、当該識別情報とオフセット値を判定部105gに引き渡す。そして、統括部105dは判定部105gに対して識別情報に係るデジタルコンテンツを内蔵HDD104から読み出すことの可否について判定を要求する。

【0051】判定部105gは、統括部105dからの要求を受け付けると、統括部105dから受け取った識別情報を取得部105jに引き渡す。そして、判定部105gは、取得部105jに対して、当該識別情報に対応する乱数を不揮発性メモリ110から読み出すと共に、当該識別情報に対応する乱数とオフセット値とを内蔵HDD104から読み出すように要求する。

【0052】取得部105jは、判定部105gからの要求を受け付けると、不揮発性メモリ110を精査して、判定部105gから受け取った識別情報に一致する識別情報が不揮発性メモリ110に記録されているか否かを調査する。その結果、当該識別情報が不揮発性メモリ110に記録されていることが確認されたら(ステップS503)、判定部105gは当該識別情報に対応する乱数を不揮発性メモリ110から読み出す(ステップS504)。

【0053】更に、取得部105jは、復号化部105iに判定部105gから受け取った識別情報を引き渡して、当該識別情報に対応する乱数とオフセット値とを内蔵HDD104から読み出し、当該乱数とオフセット値

を復号化するように要求する。復号化部105iは、取得部105jからの要求を受け付けると、内蔵HDD104を精査して、取得部105jから受け取った識別情報に対応する乱数とオフセット値とを読み出す(ステップS505)。

【0054】そして、復号化部105iは、読み出した乱数とオフセット値とを復号化した後、復号化した乱数とオフセット値とを取得部105jに引き渡す(S506)。取得部105jは、復号化部105iから乱数とオフセット値とを受け取ると、不揮発性メモリ110から読み出した乱数と併せて、これらのデータを判定部105gに引き渡す。

【0055】判定部105gは、不揮発性メモリ110から読み出した乱数と内蔵HDD104から読み出した乱数とオフセット値とを取得部105jから受け取ると、まず、不揮発性メモリ110から読み出した乱数と内蔵HDD104から読み出した乱数とを比較する。この比較の結果、不揮発性メモリ110から読み出した乱数と内蔵HDD104から読み出した乱数とが一致していたら(ステップS507: Yes)、判定部105gは、次に、統括部105dから受け取ったオフセット値と取得部105gから受け取ったオフセット値とを比較する。

【0056】この比較の結果、統括部105dから受け取ったオフセット値が取得部105gから受け取ったオフセット値以下であれば(ステップS508: Yes)、判定部105gは、前記識別情報に係るデジタルコンテンツを内蔵HDD104から読み出しても良いと判定する(ステップS509)。ステップS503、S507、S508のいずれかでNoの場合、判定部105gは、前記識別情報に係るデジタルコンテンツを内蔵HDD104から読み出すのは不可と判定する(ステップS511)。

【0057】そして、判定部105gは、上述のような判定結果を統括部105dに通知する。統括部105dは、判定部105gから判定結果の通知を受け付けると、当該判定結果をコマンド処理部103に通知して再生処理を終了する(ステップS510)。

(3) 移動処理

図6は、データ管理部105が実行する移動処理について処理の流れを示したフローチャートである。図6に示すように、データ管理部105は、コマンド処理部103からの識別情報を識別情報受付部105bにて受け付ける(ステップS701)。更に、データ管理部105は、コマンド処理部103からのオフセット値をオフセット値受付部105aにて受け付ける(ステップS702)。

【0058】統括部105dは、識別情報受付部105bから識別情報を受け取り、オフセット値受付部105aからオフセット値を受け取ると、当該識別情報とオフ

セット値を判定部105gに引き渡す。そして、統括部105dは判定部105gに対して識別情報に係るデジタルコンテンツを内蔵HDD104から読み出すことの可否について判定を要求する。

【0059】判定部105gは、統括部105dからの要求を受け付けると、統括部105dから受け取った識別情報を取得部105jに引き渡す。そして、判定部105gは、取得部105jに対して、当該識別情報に対応する乱数を不揮発性メモリ110から読み出すと共に、当該識別情報に対応する乱数とオフセット値とを内蔵HDD104から読み出すように要求する。

【0060】取得部105jは、判定部105gからの要求を受け付けると、不揮発性メモリ110を精査して、判定部105gから受け取った識別情報に一致する識別情報が不揮発性メモリ110に記録されているか否かを調査する。その結果、当該識別情報が不揮発性メモリ110に記録されていることが確認されたら(ステップS703)、判定部105gは当該識別情報に対応する乱数を不揮発性メモリ110から読み出す(ステップS704)。

【0061】更に、取得部105jは、復号化部105iに判定部105gから受け取った識別情報を引き渡して、当該識別情報に対応する乱数とオフセット値とを内蔵HDD104から読み出した後、当該乱数とオフセット値を復号化するように要求する(ステップS705)。復号化部105iは、取得部105jからの要求を受け付けると、内蔵HDD104を精査して、取得部105jから受け取った識別情報に対応する乱数とオフセット値とを読み出す(ステップS706)。

【0062】そして、復号化部105iは、読み出した乱数とオフセット値とを復号化した後、復号化した乱数とオフセット値とを取得部105jに引き渡す。取得部105jは、復号化部105iから乱数とオフセット値とを受け取ると、不揮発性メモリ110から読み出した乱数と併せて、これらのデータを判定部105gに引き渡す。

【0063】判定部105gは、不揮発性メモリ110から読み出した乱数と内蔵HDD104から読み出した乱数とオフセット値とを取得部105jから受け取ると、まず、不揮発性メモリ110から読み出した乱数と内蔵HDD104から読み出した乱数とを比較する。この比較の結果、不揮発性メモリ110から読み出した乱数と内蔵HDD104から読み出した乱数とが一致していたら(ステップS707: Yes)、判定部105gは、次に、統括部105dから受け取ったオフセット値と取得部105gから受け取ったオフセット値とを比較する。

【0064】この比較の結果、統括部105dから受け取ったオフセット値が取得部105gから受け取ったオフセット値以下であれば(ステップS708: Yes

s)、判定部105gは前記識別情報に係るデジタルコンテンツを内蔵HDD104から読み出しても良いと判定して(ステップS711)、統括部105dに判定結果を通知する(ステップS712)。

【0065】ステップS703、S707、S708のいずれかでNoの場合、判定部105gは前記識別情報に係るデジタルコンテンツを内蔵HDD104から読み出すのは不可と判定して(ステップS709)、統括部105dに判定結果を通知する(ステップS710)。統括部105dは、判定部105gから受け取った判定結果がデジタルコンテンツ読み出し可ならば、統括部105dは、当該オフセット値とデジタルコンテンツの識別情報とを記録部105fに引き渡して、内蔵HDD104と不揮発性メモリ110とに格納するように促す。記録部105fは、統括部105dから識別情報とオフセット値を受け取ると、乱数発生部105eに対して乱数を発生させるように要求する。

【0066】乱数発生部105eは、記録部105fからの要求に応じて乱数を発生させ(ステップS713)、発生させた乱数を記録部105fに引き渡す。記録部105fは、乱数発生部105eから乱数を受け取ると、当該乱数と統括部105dから受け取った識別情報とを不揮発性メモリ110に書き込む(ステップS714)。また、オフセット値受付部105aから受け取ったオフセット値を1だけ増加させる(ステップS715)。

【0067】記録部105fは、前記識別情報、乱数およびオフセット値を暗号化部105hに引き渡して内蔵HDD104に格納するように要求する。暗号化部105hは、記録部105fから受け取った識別情報、乱数およびオフセット値を暗号化する(ステップS716)。そして、暗号化部105hは、暗号化した識別情報、乱数およびオフセット値を内蔵HDD104に書き込む(ステップS717)。

【0068】そして、統括部105dは、判定部105gから判定結果の通知を受け付けると、当該判定結果をコマンド処理部103に通知する。そして、統括部105dは、コマンド処理部103から移動処理を終了させよとの指示を受け付けたかどうかを判定し、かかる指示を受け付けていなければ(ステップS718:No)、ステップS715に進んで、処理を繰り返す。従って、デジタルコンテンツの利用と並行して、逐次的、継続的にデジタルコンテンツの利用位置が内蔵HDD104に記録される。そして、統括部105dは、移動処理を終了せよとの指示を受け付けると(ステップS718:Yes)、移動処理を終了する。

【0069】以上、説明したように本実施の形態に係るデジタルテレビよれば、コピー制御情報が「Copy No More」であるようなデジタルコンテンツを内蔵HDD104から別の記録メディア(本実施の形態に

おいてはDVDを例示した。)へ移動させる際に、デジタルコンテンツの中の移動させた部分を逐次、DVDレコーダ4側に記録するので、移動元の内蔵HDD104と移動先の記録メディアの双方に同一のデジタルコンテンツが存在することによる複製品の発生を回避しながら、デジタルコンテンツの移動に際してのユーザの利便性を向上させることができる。

【0070】また、内蔵HDD104からデジタルコンテンツを読み出すのに先立って、読み出しの可否を判断するのに内蔵HDD104とは別体の不揮発性メモリ110に記録した乱数を参照するので、デジタルコンテンツの移動に先立って内蔵HDD104を取り出し、これをパーソナルコンピュータに接続してバックアップを作成し、デジタルコンテンツを移動した後にバックアップしておいたデジタルコンテンツを内蔵HDD104に戻すといった操作をされると、1のデジタルコンテンツについて内蔵HDD104に記録されている乱数と不揮発性メモリ110に記録されている乱数とが不一致となるので、内蔵HDD104からデジタルコンテンツを読み出すことが出来なくなる。従って、本発明に係るデジタルテレビによれば、デジタルコンテンツの不正コピーを防止することが出来る。

【0071】(変形例)以上、本発明を実施の形態に基づいて説明してきたが、本発明は、上述の実施の形態に限定されないのは勿論であり、以下のような変形例を実施することができる。

(1) 上記実施の形態においては、オフセット値をデジタルコンテンツ中のTSパケットの番号であるとしたが、これに代えて次のようにしても良い。例えば、TSパケット1つずつに番号を割り振る代わりに所定TSパケット数(例えば、10TSパケット。)ずつ番号を割り振って、これをオフセット値としても良い。

【0072】また、デジタルコンテンツに含まれる時間情報を参照して、先頭から所定時間分(例えば、10秒分。)毎にオフセット値を1ずつ増加させるとしても良い。更に、デジタルコンテンツの先頭から所定データ量(例えば、8キロバイト。)毎にオフセット値を1ずつ増加させるとしても良い。なお、DTCIPにはデジタルコンテンツを移動させる際に同一コンテンツの複製物が1分間以上、存続してはならないとの規定があるため、オフセット値を規定するにあたっては当該規定を遵守できる程度に細かくデジタルコンテンツを分割できるように注意するのが望ましい。

【0073】(2) 上記実施の形態においては、デジタルコンテンツの識別情報として、コマンド処理部103が前記リモートコントローラや操作パネルを介して受け付けた識別情報を用いるとしたが、これに代えて次のようにするとしても良い。すなわち、デジタルコンテンツを内蔵HDD104に格納する際に用いるファイル名であってもよいし、デジタルコンテンツ全体のハッシュ

10

20

30

40

50

値を識別情報としても良い。

【0074】或いは、ハッシュ値を識別情報とするのに代えて、デジタルコンテンツを内蔵HDD104に格納する際に行う暗号化処理に係る暗号鍵を識別情報としても良い。この場合、内蔵HDD104と不揮発性メモリ110とのそれぞれに暗号鍵を格納し、デジタルコンテンツの利用時に当該暗号鍵を照合することによって、利用の可否を判定するとしても良い。

【0075】(3) 上記実施の形態においては、デジタルコンテンツを移動する際にオフセット値を内蔵HDD104と不揮発性メモリ110とに記録するとしたが、これに加えて次のような場合にもオフセット値を記録するとしても良い。すなわち、デジタルコンテンツの部分データのうち、DVDレコーダ4に記録してから所定の時間が経過した部分データを削除する場合に、削除されずに残った部分データの先頭を示すオフセット値を記録するとしても良い。また、再生が一回しか認められていないデジタルコンテンツを再生する場合に、未だ再生されていない部分の先頭を示すオフセット値を記録するとしても良い。

【0076】(4) 上記実施の形態においては、デジタルテレビが受信したデジタルコンテンツを内蔵HDD104に記録するとしたが、これに代えて次のようにしても良い。すなわち、HDD以外の記録媒体として、例えば、メモリカードやD-VHS、DVDレコーダ等を用いてデジタルコンテンツを記録するとしてもよい。この場合、上記識別情報、オフセット値および乱数は内蔵HDD104に記録される代わりに前記メモリカード等、デジタルコンテンツを記録する記録媒体に記録される。

【0077】(5) 上記実施の形態においては、デジタルコンテンツの識別情報と乱数とを不揮発性メモリ110に記録するとしたが、これに代えて次のようにしても良い。すなわち、アクセスする際に認証が必要となる記録装置にデジタルコンテンツの識別情報と乱数とを記録するとしても良い。或いは、EEPROMや常時通電したRAM等に識別情報等を記録するとしても良い。どのような記録装置であっても、一般のユーザが自由に読み書きできなければよく、この条件さえ満たせば特に限定されるものではない。

【0078】(6) 上記実施の形態においては、デジタルコンテンツを内蔵HDD104からDVDレコーダ4へ移動させるとしたが、これに代えて次のようにしても良い。すなわち、DVDレコーダ以外のデジタル記録可能な記録媒体、例えば、メモリカードやD-VHS、HDDレコーダ等に対して内蔵HDD104からデジタルコンテンツを移動させるとしても良い。

【0079】(7) 上記実施の形態においては、乱数を内蔵HDD104に記録する際に暗号化部105hにて暗号化し、内蔵HDD104から読み出す際に復号化

部105iにて復号化した後に、不揮発性メモリ110に記録されていた乱数と比較するとしたが、これに代えて次のようにしても良い。すなわち、乱数を内蔵HDD104に記録する際に、これを一方方向関数により変換した結果を記録するとし、内蔵HDD104から読み出す際には復号化は行なわない。また、不揮発性メモリ110には乱数をそのまま記録することとし、これを読み出す際に併せて前記一方方向関数を用いて変換するものとする。そして、内蔵HDD104から読み出された変換結果と、不揮発性メモリ110から読み出された乱数の変換結果とを比較することによって、対応するデジタルコンテンツの読み出しの可否を判定するとしても良い。

【0080】また、これとは逆に、不揮発性メモリ110には乱数を一方方向関数により変換した結果を記録し、内蔵HDD104には乱数をそのまま記録することとし、内蔵HDD104から読み出す際には同じ一方方向関数を用いて変換するものとしても良い。このようにしても、上と同様の効果を得ることができる。また、後述のように、デジタルコンテンツのハッシュ値を識別情報とするような場合には、内蔵HDD104と比較して記憶容量の制限が厳しい不揮発性メモリ110に格納すべき識別情報のデータ量を小さくすることができるので有効である。

【0081】(8) 上記実施の形態においては、本発明をデジタルテレビ1に適用するとしたが、これに代えて次のようにしても良い。すなわち、デジタル放送を受像するためにテレビに接続するセットトップボックスに本発明を適用するとしても良い。図7は、本発明を適用したセットトップボックスの概略構成を示す機能ブロック図である。

【0082】図7に示すように、セットトップボックス7は、上記実施の形態に係るデジタルテレビ1と概ね同様の構成を備えているが、デジタルテレビ1がモニタ部106を内蔵しているのに対して、セットトップボックス7はアナログハイビジョンテレビがコンポーネントケーブルを介して接続されていることを主たる特徴とする。

【0083】セットトップボックス7は、デジタルテレビ1と同様に、BSアンテナ6にて放送衛星5からのBSデジタル放送を受信すると、チューナ部6にて復調したデジタルコンテンツを、コマンド処理部704にて受け付けたユーザの指定に応じて、暗号処理部705にて暗号化した上で内蔵HDD709に記録する。この際、セットトップボックス7は、上記実施の形態におけるのと同様に、内蔵HDD709と不揮発性メモリ707との双方に当該デジタルコンテンツの識別情報等を記録する。

【0084】セットトップボックス7は、また、コマンド処理部704にて受け付けたユーザの指定に応じて、内蔵HDD709からデジタルコンテンツを読み出し、

暗号処理部 705 にて復号化する。そして、セットトップボックス 7 は、復号化したデジタルコンテンツを、MPEG デコーダ 703 を介し、アナログハイビジョンテレビ 8 に向けて出力する。この場合も、セットトップボックス 7 は、上記実施の形態におけるのと同様に、内蔵 HDD 709 と不揮発性メモリ 707 との双方に当該デジタルコンテンツの識別情報等を照合して、当該デジタルコンテンツを内蔵 HDD 709 から読み出すことの可否を判定する。

【0085】 以上のように、本発明をセットトップボックスに適用した場合においても、上記実施の形態におけるのと同様の効果を得ることができる。すなわち、セットトップボックスに記録されているデジタルコンテンツのバックアップを作成し、セットトップボックスから別の記録媒体にデジタルコンテンツを移動させた後に、当該バックアップをセットトップボックスの内蔵 HDD にコピーすることにより、デジタルコンテンツの不正コピーを作成することを防止することができる。

【0086】 (9) 上記実施の形態においては、デジタルコンテンツ中の読み出し開始位置をオフセット値として内蔵 HDD 104 に記録するとしたが、これに代えて次のようにしても良い。すなわち、上記実施の形態においては、まず、(a) オフセット値を増加させてから (ステップ S 715)、(b) 識別情報、乱数及びオフセット値を暗号化し (ステップ S 716)、(c) 暗号化した識別情報、乱数及びオフセット値を内蔵 HDD 104 に記録する (ステップ S 717) としたが、これに代えて、まず、(a') 識別情報、乱数及びオフセット値を暗号化し、(b') 暗号化した識別情報、乱数及びオフセット値を内蔵 HDD 104 に記録してから、(c')

オフセット値を増加させるとしても良い。

【0087】 このようにすれば、内蔵 HDD 104 には、常にデジタルコンテンツ中の利用済みの部分の末尾位置、すなわち、末尾位置が記録されることになるので、デジタルコンテンツを内蔵 HDD 104 から他の記録媒体に移動させている途中で電源が杜絶する等の原因により移動処理が中断した場合であっても、後に、処理を再開した際に移動処理が未了の箇所からデジタルコンテンツを利用することができるので、ユーザにとって利便性が高い。

【0088】 また、このようにした場合であっても、頻繁に書き換えが発生するオフセット値の書き込みを内蔵 HDD 104 に対してのみ行い、不揮発性メモリ 110 に対してはオフセット値を書き込まないので、不揮発性メモリ 110 がフラッシュメモリのように書き込み回数に制限のあるメモリであるような場合には、特に、有効である。

【0089】 また、この場合、オフセット値を暗号化して記録するとすれば、デジタルコンテンツの利用箇所の末尾位置を分かり難くすることができるので、例えば、

内蔵 HDD 104 を取り出してパーソナルコンピュータに接続し、末尾位置の記録を改竄することによってデジタルコンテンツの不正コピーを行うといった不正利用を防止することができる。従って、末尾位置を不揮発性メモリ 110 に記録しなくとも、末尾位置の改竄による不正コピーの防止を実現することができる。

【0090】 なお、上記のオフセット値は、前述の変形例 (1) にて説明したように、1 TS パケット毎に制限されない。例えば、10 TS パケット毎にオフセット値を記録するような場合には、1 番目の TS パケットや 11 番目の TS パケット、21 番目の TS パケット等が利用位置の先頭となる訳だが、このような場合、末尾位置として 0、10、20 等が順に記録される。

【0091】 (10) 本発明はコンピュータに上記のような処理を実行させるプログラムであるとしてもよい。このようにすれば、コンピュータに上記のようなデジタルコンテンツの管理をさせることによって、上記と同様の効果を得ることができる。

【0092】

【発明の効果】 以上説明したように、本発明に係るデジタルコンテンツ管理装置は、デジタルコンテンツと当該デジタルコンテンツに対応する管理情報とを記録する第 1 の記録手段と、前記管理情報を記録する第 2 の記録手段と、デジタルコンテンツの利用に先立って、前記第 1 の記録手段にて記録されている管理情報と前記第 2 の記録手段にて記録されている管理情報とを照合して、前記デジタルコンテンツの利用の可否を判定する管理情報判定手段と、前記管理情報判定手段にて利用可と判定されたデジタルコンテンツが利用されるに際して、前記第 1 の記録手段にて記録されている管理情報と前記第 2 の記録手段にて記録されている管理情報とを変更する管理情報更新手段とを備えるとするので、例えば、デジタルテレビの内蔵 HDD にデジタルコンテンツが記録されている場合に、当該内蔵 HDD 全体のバックアップを作成しておき、前記デジタルコンテンツを DVD-ROM 等へ移動させた後に、バックアップしておいたデータを前記内蔵 HDD に戻す操作がされたか否かを検出して、当該操作が検出された場合には前記内蔵 HDD に記録されている前記デジタルコンテンツの利用を禁止することができるので、不正な利用を防止することが出来る。

【0093】 また、本発明に係るデジタルコンテンツ管理装置は、前記第 1 の記録手段にて記録する管理情報を暗号化する管理情報暗号化手段と、前記第 1 の記録手段から読み出された管理情報を復号化する管理情報復号化手段とを備え、前記第 1 の記録手段は、前記管理情報暗号化手段にて暗号化された管理情報を記録し、前記管理情報判定手段は、前記管理情報復号化手段にて復号化された管理情報を用いて前記照合を行なうので、管理情報が改竄され難くなり、不正コピーの防止を更に強化することができる。

【0094】また、上記に代えて、前記第1の記録手段にて記録する管理情報を符号化する第1の符号化手段と、前記第2の記録手段から読み出された管理情報を符号化する第2の符号化手段とを備え、前記第1の記録手段は、前記第1の符号化手段にて符号化された管理情報を記録し、前記管理情報判定手段は、前記第2の符号化手段にて符号化された管理情報を用いて前記照合を行なうので、やはり管理情報の不正な改竄が困難となつて、不正コピーの防止を強化することができる。

【0095】また、前記第1の記録手段から読み出された管理情報を符号化する第1の符号化手段と、前記第2の記録手段にて記録する管理情報を符号化する第2の符号化手段とを備え、前記第2の記録手段は、前記第2の符号化手段にて符号化された管理情報を記録し、前記管理情報判定手段は、前記第1の符号化手段にて符号化された管理情報を用いて前記照合を行なうので、上記の効果に加えて前記第2の記録手段にて記録すべきデータ量を削減することができる。したがって、前記第2の記録手段としてHDD等との比較において記憶容量のより小さい半導体メモリ等を用いる場合に有効である。

【0096】また、本発明に係るデジタルコンテンツ管理装置は、デジタルコンテンツ中の利用位置を取得する位置取得手段と、デジタルコンテンツ中の利用位置の末尾位置を記録する末尾位置記録手段と、前記末尾位置記録手段にて記録されているデジタルコンテンツ中の利用位置の末尾位置と、位置取得手段にて取得されたデジタルコンテンツ中の利用位置とを比較して、デジタルコンテンツの利用の可否を判定する位置判定手段と、前記管理情報判定手段と前記位置判定手段とがデジタルコンテンツを利用可と判定したときのみ、デジタルコンテンツを利用可と判定する最終判定手段とを備えているので、デジタルコンテンツの移動済み部分を確実に記録することができる。

【0097】従つて、コピー制御情報として「Copy One Generation」を付加されているデジタルコンテンツを一の記録媒体から別の記録媒体へ移動させる場合に、移動を中断させても当該デジタルコンテンツの未移動の部分が無効にされることがなく、複製品を許さないというDTCFの趣旨を逸脱せずにユーザの利便性を向上させることができる。

【0098】また、例えば、内蔵HDDにデジタルコンテンツを記録するHDDレコーダに対し本発明を適用する場合、第一の記録手段が前記内蔵HDDへ記録を行い、第二の記録手段が不揮発性メモリへ記録を行なうとし、前記利用位置やその末尾位置を前記内蔵HDDに記録すれば、不揮発性メモリへの書き込み回数を最小限に留めることができると共に、デジタルコンテンツの利用位置を確実に逐次記録することができる。

【0099】また、デジタルコンテンツの移動が電源断等を原因として中断したとしても、次回の移動で中断し

た時点の続きから再開することができる。また記録された利用位置の改竄を判定できるため、不正コピーを防止しながら、同時にユーザの利便性を向上させることができる。また、前記末尾位置記録手段は、前記第1の記録手段にて前記デジタルコンテンツ中の利用位置の末尾位置を記録するので、前記第2の記録手段がフラッシュメモリのように書き込み回数に制限のある記憶装置であるような場合に、斯かる記憶装置に対する書き込み回数を削減することができる。

【0100】また、前記末尾位置記録手段は、前記デジタルコンテンツ中の利用位置の末尾位置を暗号化して記録するので、前記第1の記憶手段がHDDのように記録内容を不正に読み出すことが可能であるような場合に、読み出した利用位置の解読を困難とすることができるので、デジタルコンテンツの不正利用を防止することができる。

【0101】なお、デジタルコンテンツの利用位置を記録するにあたっては、例えば、前記デジタルコンテンツは1以上の部分データからなっており、前記デジタルコンテンツ中の利用位置は、前記デジタルコンテンツの先頭からの前記部分データの順序情報により示されることができる。また、本発明に係るデジタルコンテンツ管理装置は、乱数を発生させる乱数発生手段を備え、前記管理情報は前記乱数発生手段が発生させた乱数を含んでいるので、単にデジタルコンテンツの利用回数を管理情報とする場合と比較して、デジタルコンテンツの不正利用者による管理情報の改竄がより困難となるので、不正コピーの防止を強化することができる。

【0102】また、本発明に係るデジタルコンテンツ管理装置は、前記デジタルコンテンツを識別する識別情報を取得する識別情報取得手段を備え、前記管理情報は前記識別情報を含んでいるので、例えば、デジタルテレビの内蔵HDDに格納されているデジタルコンテンツを別のデジタルコンテンツに書き換える操作がされたか否かを検出して、当該別のデジタルコンテンツが不正に利用されるのを防止することができる。

【0103】なお、前記識別情報は、対応するデジタルコンテンツのハッシュ値を含み、前記第1の記録手段から読み出したデジタルコンテンツのハッシュ値と前記第2の記録手段から読み出した管理情報に含まれているハッシュ値を照合してデジタルコンテンツの利用の可否を判定するハッシュ値照合手段を備えているので、デジタルコンテンツの書き換えがされたか否かを検出することができ、上述のような不正利用をより確実に検出して、これを防止することができる。

【0104】また、前記第1の記録手段は、前記デジタルコンテンツを暗号鍵を用いて暗号化して記録し、前記識別情報は、前記暗号鍵を含み、前記第1の記録手段から読み出した前記識別情報に含まれている暗号鍵と前記第2の記録手段から読み出した前記識別情報に含まれて

10

20

30

40

50

いる暗号鍵とを照合してデジタルコンテンツの利用の可否を判定する暗号鍵照合手段を備えているので、識別情報のデータサイズを低減することができ、前記第1の記録手段および前記第2の記録手段においてデジタルコンテンツの管理に要する記録容量を低減して、コストを削減することができる。

【0105】また、本発明に係るデジタルコンテンツ管理装置は、前記第2の記録手段は不揮発性メモリであることにによって、内蔵HDD等の記録媒体に管理情報を記録する場合と比較して、前記第2の記録手段にて記録された管理情報の読み出しや改竄がより困難となるので、デジタルコンテンツの不正利用の防止を強化することができる。

【0106】また、本発明に係るデジタルコンテンツ管理プログラムは、デジタルコンテンツと当該デジタルコンテンツに対応する管理情報とを記録する第1の記録ステップと、前記管理情報を記録する第2の記録ステップと、前記デジタルコンテンツが利用される際に、前記第1の記録ステップにて記録された管理情報と前記第2の記録ステップにて記録された管理情報とを更新する管理情報更新ステップと、前記第1の記録ステップにて記録された管理情報と前記第2の記録ステップにて記録された管理情報とを照合して、前記デジタルコンテンツの利用の可否を判定する管理情報判定ステップとを備えているので、上述のデジタルコンテンツ管理プログラムと同様に、デジタルコンテンツの不正な利用を防止することが出来る。

【0107】また、本発明に係るデジタルコンテンツ管理プログラムは、前記第1の記録ステップにて記録する管理情報を暗号化する管理情報暗号化ステップと、前記第1の記録ステップにて記録された管理情報を復号化する管理情報復号化ステップとを備えており、或いはこれに代えて、前記第1の記録ステップにて記録する管理情報を符号化する第1の符号化ステップと、前記第2の記録ステップにて記録された管理情報を符号化する第2の符号化ステップとを備えているので、管理情報を改竄され難くして不正コピーを防止することができる。

【0108】また、前記第1の記録ステップにて記録された管理情報を符号化する第1の符号化ステップと、前記第2の記録ステップにて記録する管理情報を符号化する第2の符号化ステップとを備えているので、やはり管理情報を改竄され難くして不正コピーを防止することができる。また、本発明に係るデジタルコンテンツ管理プログラムは、デジタルコンテンツの利用位置を取得する位置取得ステップと、デジタルコンテンツの利用位置の末尾位置を記録する末尾位置記録ステップと、前記末尾位置記録ステップにて記録されたデジタルコンテンツの利用位置の末尾位置と、位置取得ステップにて取得されたデジタルコンテンツの利用位置とを比較して、デジタルコンテンツの利用の可否を判定する位置判定ステップ

と、前記管理情報判定ステップと前記位置判定ステップとがデジタルコンテンツを利用可と判定したときのみ、デジタルコンテンツを利用可と判定する最終判定ステップとを備えているので、上述のように電源断等起因するデジタルコンテンツの移動処理の中断によるデジタルコンテンツの損失を防止して、ユーザの利便性を向上させることができる。

【0109】また、前記末尾位置記録ステップは、前記デジタルコンテンツ中の利用位置の末尾位置を暗号化して記録するので、不正に末尾位置を読み出して改竄することによるデジタルコンテンツの不正利用を防止することができる。また、このとき更に、前記デジタルコンテンツは1以上の部分データからなっており、前記デジタルコンテンツの利用位置は、前記デジタルコンテンツの先頭からの前記部分データの順序情報により示されるので、上に述べたように、複製品を許さないというDTCPの趣旨を逸脱せずにユーザの利便性を向上させることができる。

【0110】また、本発明に係るデジタルコンテンツ管理プログラムは、前記管理情報として乱数を発生させる乱数発生ステップを備えているので、デジタルコンテンツの不正な利用を防止することができる。また、本発明に係るデジタルコンテンツ管理プログラムは、前記デジタルコンテンツを識別する識別情報を取得する識別情報取得ステップを備え、前記管理情報は前記識別情報を含んでいるので、デジタルコンテンツの書き換えによる不正利用を防止することができる。

【0111】なお、デジタルコンテンツの書き換えがされたか否かを検出するには、これに加えて、例えば、前記識別情報は、対応するデジタルコンテンツのハッシュ値を含み、前記第1の記録ステップにて記録されたデジタルコンテンツのハッシュ値と前記第2の記録ステップにて記録された管理情報に含まれているハッシュ値を照合してデジタルコンテンツの利用の可否を判定するハッシュ値照合ステップを備えることによって、上述のような不正利用をより確実に検出して、これを防止することができる。

【0112】また、前記第1の記録ステップは、前記デジタルコンテンツを暗号鍵を用いて暗号化して記録し、前記識別情報は、前記暗号鍵を含み、前記第1の記録ステップにて記録された前記識別情報に含まれている暗号鍵と前記第2の記録ステップにて記録された前記識別情報に含まれている暗号鍵とを照合してデジタルコンテンツの利用の可否を判定する暗号鍵照合ステップを備えているので、これによってもデジタルコンテンツの不正利用を防止することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係るデジタルテレビの概略構成を示す機能ブロック図である。

【図2】デジタルテレビ1が備えているデータ管理部1

10

20

30

40

50

05について、その概略構成を示す機能ブロック図である。

【図3】データ管理部105の動作について、そのメインルーチンを示すフローチャートである。

【図4】データ管理部105が実行する記録処理について、処理の流れを示したフローチャートである。

【図5】データ管理部105が実行する再生処理について、処理の流れを示したフローチャートである。

【図6】データ管理部105が実行する移動処理について、処理の流れを示したフローチャートである。

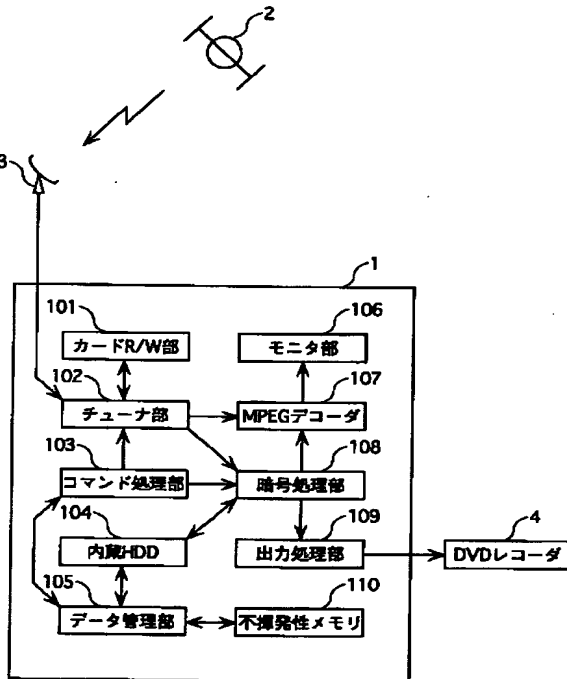
【図7】変形例(8)に係るセットトップボックスの概略構成を示す機能ブロック図である。

【符号の説明】

- 1 デジタルテレビ
- 2 放送衛星
- 3 BSデジタル用アンテナ
- 4 DVDレコーダ
- 101 カードR/W部
- 102 チューナ部
- 103 コマンド処理部
- 104 内蔵HDD
- 105 データ管理部
- 106 モニタ部
- 107 MPEGデコーダ
- 108 暗号処理部
- 109 出力処理部
- 110 不揮発性メモリ

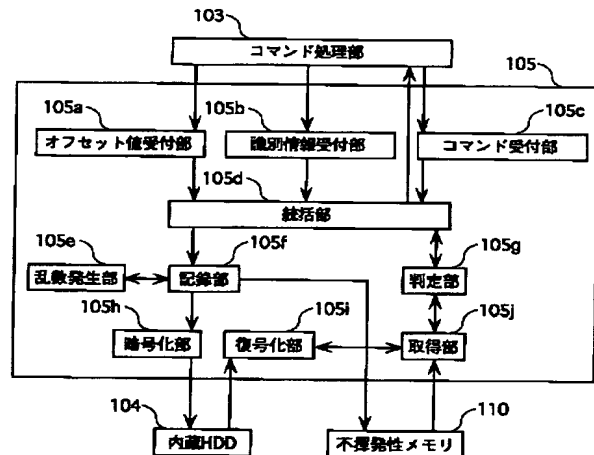
*

【図1】

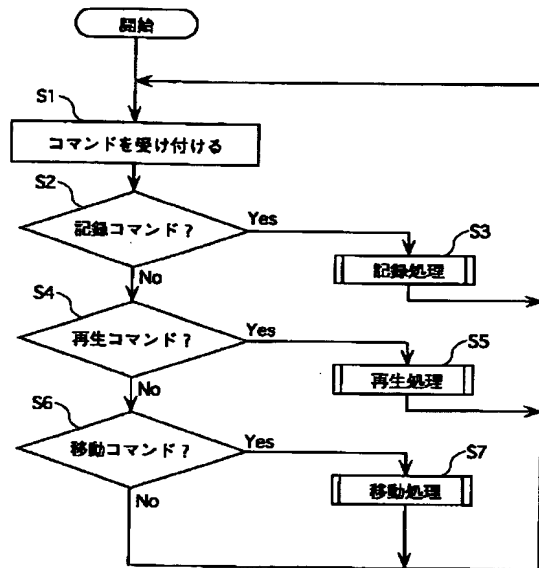


- * 103 コマンド処理部
- 104 内蔵HDD
- 105 データ管理部
- 105a オフセット値受付部
- 105b 識別情報受付部
- 105c コマンド受付部
- 105d 統括部
- 105e 乱数発生部
- 105f 記録部
- 105g 判定部
- 105h 暗号化部
- 105i 復号化部
- 105j 取得部
- 106 モニタ部
- 107 MPEGデコーダ
- 108 暗号処理部
- 109 出力処理部
- 110 不揮発性メモリ

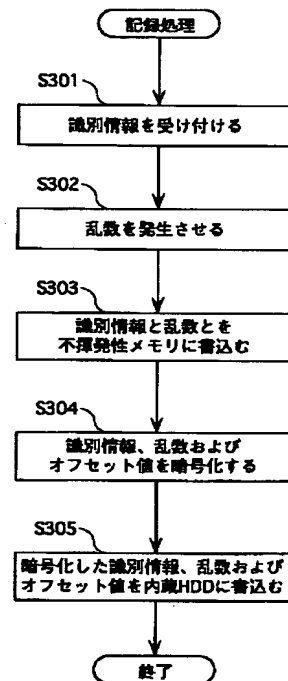
【図2】



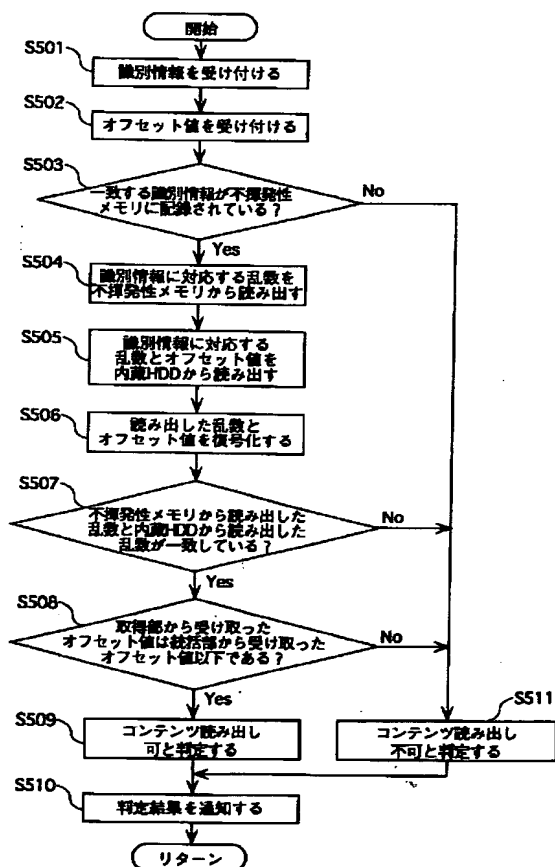
【図3】



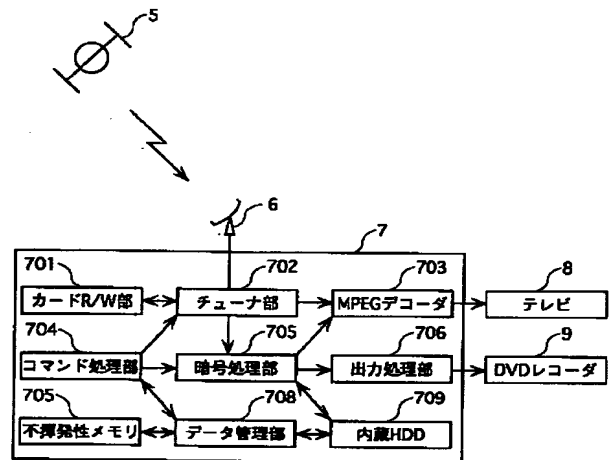
【図4】



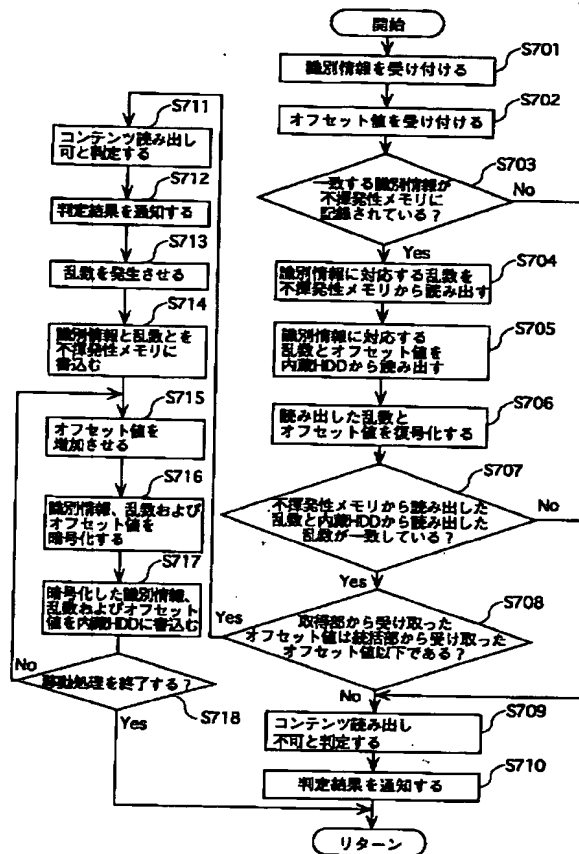
【図5】



【図7】



【図6】



フロントページの続き

Fターム(参考) 5B017 AA06 BA07 CA07
 5D044 AB05 AB07 BC01 BC04 CC04
 CC09 DE49 DE50 EF05 FG18
 GK12 GK17 HL08
 5J104 AA08 AA13 AA16 NA02 NA12
 PA05